In the Claims:

1. (currently amended) A N-dimensional biometric security system comprising

a station for receiving information representative of a user from the user and generating a signal responsive thereto;

a first data base having a plurality of words and language rules for randomly generating one-time challenge phrases wherein each word is randomly generated;

a second data base having biometric models of the user therein; and

a controller to receive and validate said signal as representative of the user, said controller, in response to validation of said signal, communicating with said first data base for randomly generating a one-time challenge phrase from said plurality of words and language rules in said first data base and delivering said one-time challenge phrase to said station for the user to speak said one-time challenge phrase exactly ~~in response to validation of said signal~~, and said controller communicating with said station

to receive a spoken response from the user to said delivered one-time challenge phrase and to generate a second signal representative of the spoken response,

to process the entire said second signal for speaker recognition and to issue a first validation signal in response to a match between said second signal and said stored biometric model,

to process the entire said second signal for speech recognition and to issue a second validation signal in response to said second signal exactly matching said one-time challenge phrase, and

to validate the spoken response to said one-time challenge phrase as representative of the user in response to receiving said first validation signal and said

second validation signal.

2. (currently amended) A method of identifying and validating a user comprising the steps of

initially inputting information representative of the user at a station;

generating a first signal responsive to the information;

receiving and validating said first signal as representative of the user;

thereafter, in response to validation of said first signal, generating and delivering a randomly generated one-time challenge phrase wherein each word of said phrase is randomly generated at said station for the user to speak exactly;

generating a second signal representative of a spoken response to said challenge phrase;

thereafter receiving and simultaneously processing the entire second signal for each of speaker verification and ~~for~~ speech recognition and issuing a first validation signal in response to speaker verification and a second validation signal in response to speech recognition; and

validating the second signal as representative of the user in response to issuance of said first validation signal and said second validation signal.

3. (canceled)

4. (currently amended) A N-dimensional biometric security system comprising

a station for receiving input information representative of a user from the user and generating a first signal responsive thereto;

a first data base for storing a plurality of words and language rules for randomly generating one-time challenge phrases wherein each word of said phrase is randomly

generated ;

a second data base for storing a biometric model of the user; and

a controller for receiving and validating said first signal as representative of the user, said controller being operatively connected to said first data base to, in response to said first signal, generate and deliver a one-time randomly generated challenge phrase to said station ~~in response to said first signal~~ for the user to speak exactly,

said controller communicating with said station to receive and compare a spoken response to said challenge phrase with said entire challenge phrase to verify said spoken response as exactly matching said entire challenge phrase and to compare said spoken response to said stored biometric model of said user and for validating said spoken response as representative of said user in response to a match between said spoken response and said stored biometric model of said user, said controller issuing an authentication signal in response to a verification of said spoken response as exactly matching said challenge phrase and a validation of said spoken response as representative of said user.

5. (currently amended) A method of identifying and validating a user comprising the steps of

storing a plurality of words and language rules for randomly generating challenge phrases in a first data base;

storing a biometric model of each of a multiplicity of users in a second data base;

receiving information representative of a user from the user at an input station and generating a first signal responsive thereto;

thereafter, in response to said first signal, randomly generating a one-time

challenge phrase wherein each word of said phrase is randomly generated from said stored plurality of words and language rules and forwarding said one-time challenge phrase to said station for the user to speak exactly;

receiving a spoken response to said one-time challenge phrase;

comparing said spoken response to said entire one-time challenge phrase to verify said spoken response as exactly matching said one-time challenge phrase;

comparing said spoken response to the stored biometric models to obtain a match between said spoken response and one of said stored biometric models,

issuing a validation signal in response to a match between said spoken response and one of said stored biometric models; and

issuing an authentication signal in response to a verification of said spoken response as matching said one-time challenge phrase and issuance of said validation signal.

6. (previously presented) A method as set forth in claim 5 wherein a user additionally selects a word phrase as a private and personal challenge phrase.

7. (previously presented) A method as set forth in claim 2 wherein a user additionally selects a word phrase as a private and personal challenge phrase.

8. (previously presented) A method as set forth in claim 2 further comprising the step of establishing a session time out limit in response to said first signal.

9. – 10. (canceled)

11. (previously presented) A method as set forth in claim 5 further comprising the step of establishing a session time out limit in response to said first signal.

12.-13. (canceled)

14. (previously presented) A method as set forth in claim 5 further comprising the steps of encrypting and digitally signing said spoken response to said one-time challenge phrase after reception thereof and subsequently decrypting said spoken response prior to said step of comparing said spoken response to the stored biometric models.

15. (canceled)

16. (currently amended) A speech N-dimensional biometric security system comprising

a first data base having a plurality of words and language rules for generating randomly determined one-time challenge phrases;

a second data base having a biometric model of an authorized user;

a station for receiving information indicative of a user and generating a first signal responsive thereto; and

a controller connected to said first data base to, in response to said first signal, randomly generate a one-time challenge phrase wherein each word of said phrase is randomly generated from said plurality of words and language rules in said first data base ~~in response to said first signal~~ and to deliver said one-time challenge phrase to said station for the user to speak said one-time challenge phrase exactly, and

said controller communicating with said station to receive a spoken response from the user of said delivered one-time challenge phrase

to process said entire spoken response for biometric speaker recognition and to produce a first validation signal as representative of an authorized user in response to a match between said spoken response and said stored biometric model for an authorized user, and

to simultaneously process said entire spoken response for speech recognition

and to produce a second validation signal in response to said spoken response exactly matching said one-time challenge phrase, and

said controller to issue a positive authentication signal as representative of an authorized user in response to said first validation signal and said second validation signal being simultaneously produced.

17. (currently amended) A speech N-dimensional biometric security system comprising

a station for receiving information indicative of a present user and generating a first signal responsive thereto;

a first data base having a plurality of words and language rules for randomly generating one-time challenge phrases;

a second data base having a plurality of biometric models, each said biometric model corresponding to a respective one of a plurality of authorized users; and

a controller to receive said first signal as indicative of the present user,

said controller communicating with said first data base for randomly generating a one-time challenge phrase wherein each word of said phrase is randomly generated from said plurality of words and language rules in said first data base and delivering said one-time challenge phrase to said station for the present user to speak said one-time challenge phrase exactly, and

said controller communicating with said station to receive a spoken response from the present user of said delivered one-time challenge phrase

to process said entire spoken response for biometric speaker recognition and to produce a first validation signal as representative of said present user being an authorized user in response to a match between said spoken response and said stored

biometric model for said present user,

to simultaneously process said spoken response for speech recognition and to produce a second validation signal as representative of said spoken response exactly matching said one-time challenge phrase, and

said controller to issue a positive authentication signal as representative of said present user being an authorized user in response to said first validation signal and said second validation signal being simultaneously produced.

18. (previously presented) A N-dimensional biometric security system as set forth in claim 4 wherein said first data base stores said plurality of words and language rules in a plurality of language sets, each said language set being specific to a subject area different from the subject areas of the other of said language sets.